

This Page Is Inserted by IFW Operations  
and is not a part of the Official Record

## **BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

**IMAGES ARE BEST AVAILABLE COPY.**

As rescanning documents *will not* correct images,  
please do not report the images to the  
Image Problem Mailbox.

5

(19)日本国特許庁 (JP)

## (12) 公開特許公報 (A)

(11)特許出願公開番号

特開平8-255132

(43)公開日 平成8年(1996)10月1日

(51) Int.Cl. <sup>6</sup> G 06 F 15/00 3/14	識別記号 330 350	序内整理番号 9364-5L	F I G 06 F 15/00 3/14	技術表示箇所 330 A 350 A
---	--------------------	-------------------	-----------------------------	--------------------------

審査請求 未請求 請求項の数9 OL (全15頁)

(21)出願番号 特願平7-261144

(22)出願日 平成7年(1995)10月9日

(31)優先権主張番号 321644

(32)優先日 1994年10月11日

(33)優先権主張国 米国(US)

(71)出願人 390009531

インターナショナル・ビジネス・マシーンズ・コーポレイション

INTERNATIONAL BUSINESS MACHINES CORPORATION

アメリカ合衆国10504、ニューヨーク州

アーモンク (番地なし)

(72)発明者 マーク・アーウィン・カーソン

アメリカ合衆国20953 メリーランド州ロ

ックヴィル ジュディス・ストリート

4317

(74)代理人 弁理士 合田 澄 (外2名)

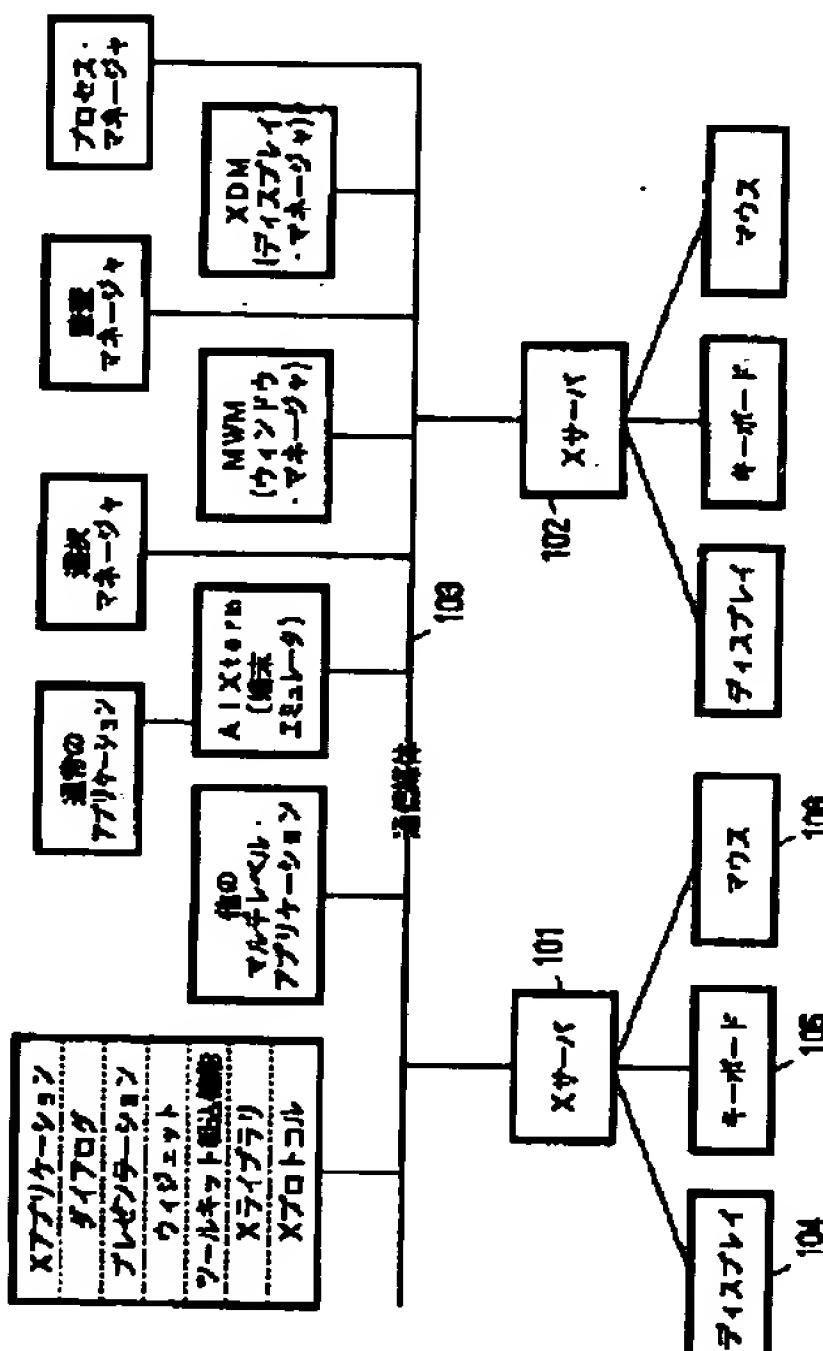
最終頁に続く

(54)【発明の名称】 安全なデータ転送を行うための方法および機密レベル変更選択機構

(57)【要約】 (修正有)

【課題】 未承認のウインドウ・システム・クライアント・プログラムが選択マネージャという特殊承認クライアント・プログラムによって仲介されてユーザの制御下で安全保護領域間でデータを転送できるようにする。

【解決手段】 使用する機構は、機密レベル変更カット・アンド・ペースト操作に関するコンパートメント化モード・ワークステーション(CMW)要件の機能を満たすように構成することができる。CMWのカット・アンド・ペースト要件を満たし、機密レベル変更選択機構が抜け道として機能するのを防止するため、この機密レベル変更選択機構では、必須アクセス管理(MAC)上位移行操作中の低レベル・プロセスへの通信にダミー・ウインドウIDを使用し、すべての機密レベル変更操作について、転送の続行を許可する前にユーザ確認を要求するポップアップを表示するよう選択マネージャに指示する。この選択機構は、カット・アンド・ペースト用の構成可能な機密レベル変更選択操作をサポートする。



## 【特許請求の範囲】

【請求項1】安全なウィンドウ・システム用の機密レベル変更選択機構において、前記ウィンドウ・システム上の個別のウィンドウで動作し、それぞれがそのウィンドウ内にデータを表示する、複数のクライアント・プログラムと、あるクライアント・プログラム・ウィンドウから別のクライアント・プログラム・ウィンドウにデータを転送するためのカット・アンド・ペースト操作用の選択マネージャというクライアントとを含み、前記選択マネージャがコンパートメント化モード・ワークステーション(CMW)要件を満たし、状態の変化をアプリケーションに通知するためにアプリケーションに事象を送信し、前記選択マネージャが転送中のデータの所有権および他の安全保護プロパティを操作して、制御式検査可能データ転送の実行を可能にすることを特徴とする、機密レベル変更選択機構。

【請求項2】必須アクセス管理(MAC)上位移行操作中の低レベル・プロセスへの通信時に、前記ウィンドウ・システムがダミーのウィンドウIDを使用することを特徴とする、請求項1に記載の機密レベル変更選択機構。

【請求項3】すべての機密レベル変更操作について、選択項目が転送される前に前記ウィンドウ・システムが前記選択マネージャに事象を送信し、その結果、転送続行が許可される前にユーザ確認を要求するポップアップを選択マネージャが表示することを特徴とする、請求項1に記載の機密レベル変更選択機構。

【請求項4】安全なウィンドウ・システム内で安全保護属性を有するデータを安全に転送する方法において、データへのアクセスに関する事前定義安全保護レベルを有する要求側からデータ転送に関する要求をウィンドウ・システムが受け取るステップと、要求側によって指定されたウィンドウIDとプロパティIDが選択側所有者から隠されて、要求側が必須アクセス管理(MAC)上位移行時に低レベル・プロセスと通信するときに選択項目の所有者が要求側に関する安全保護関連情報を入手できないようにするために、特殊なウィンドウが選択項目所有者からアクセス可能になる、前記ウィンドウ・システム上で動作する選択マネージャというクライアント・プログラムが、選択項目所有者の安全保護属性を継承する特殊なウィンドウとプロパティを作成するステップとを含むことを特徴とする、安全なデータ転送方法。

【請求項5】前記選択項目所有者が前記選択マネージャに選択項目データを転送するステップであって、転送が完了するまで前記選択マネージャがデータの所有者になり、それに対する排他的権利を有するステップと、前記選択項目所有者から選択項目要求側に転送されるデータをログイン・ユーザが検査できるようにし、機密

レベル変更操作について、データ転送の続行が許可される前にユーザ確認を要求するユーザ・インターフェースを提供するステップとをさらに含むことを特徴とする、請求項4に記載の安全なデータ転送方法。

【請求項6】MAC下位移行の使用にかかる操作を試みた場合およびデータ転送および再分類にかかる安全保護違反を犯した場合に監査事象を生成するステップをさらに含むことを特徴とする、請求項5に記載の安全なデータ転送方法。

【請求項7】要求側のウィンドウとプロパティに対する任意アクセス制御(DAC)書き込みアクセス制限を指定変更するために十分な特権を有する選択機構を提供するステップをさらに含むことを特徴とする、請求項6に記載の安全なデータ転送方法。

【請求項8】選択項目要求側と選択項目所有者との間で安全なウィンドウ・システム内で安全保護属性を有するデータを安全に転送する方法において、前記選択項目要求側がウィンドウ・システムを動作させる選択マネージャというクライアントに転送される要求を出すステップと、

前記選択マネージャが必須アクセス管理(MAC)ダイアログと任意アクセス制御(DAC)ダイアログを表示するステップと、後で選択項目の所有者が選択項目をポストすることができる専用のウィンドウ上で前記選択マネージャがプロパティを作成し、選択項目要求を生成し、最初に意図した受信側として前記選択項目所有者に前記選択項目要求を送信するステップと、

前記選択項目要求に応答して、前記選択項目所有者が前記選択マネージャのプロパティ上で選択項目データをポストし、前記選択マネージャに選択通知事象を出すステップと、

ユーザが未修正通過の要求を許可するか、要求を取り消すか、または転送中のデータを下位移行できるように、前記選択項目所有者から前記選択項目要求側に渡されるデータをユーザが検査できるようにするステップと、ユーザが要求を取り消した場合に監査事象を生成するステップと、

前記選択マネージャがそれ自体のウィンドウ/プロパティから前記選択項目要求側のウィンドウ/プロパティに選択項目データを転送し、そのプロパティ上の前記選択項目の可用性に関する通知を要求側に出すステップと、前記選択項目要求側がデータを読み取り、前記選択マネージャに通知を出すステップと、

前記選択マネージャがデータ転送の完了を所有者に通知するステップとを含むことを特徴とする、安全なデータ転送方法。

【請求項9】前記選択マネージャによる前記転送ステップが増分式に実行され、それぞれの転送ごとに個別にレベルを付けるかどうかを指定するようユーザに要求する

ステップをさらに含むことを特徴とする、請求項8に記載の安全なデータ転送方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、一般的に、コンピュータ・ウィンドウ・システム内でのカット・アンド・ペースト操作によるデータ転送に関し、より詳細には、未承認ウィンドウ・システム・クライアント・プログラムが特殊なクライアント・プログラムによって仲介される転送によってユーザの制御下でユーザの示唆により安全保護領域間でデータを転送できるようにするための安全な手段に関する。

【0002】

【従来の技術】コンピュータ・システムでは、ユーザにグラフィカル・ユーザ・インターフェース（GUI）を提供してマルチタスクのコンピュータ・プログラムを管理するために、ウィンドウ・システムが一般に使用されている。通常、コンピュータ上で現在実行されているコンピュータ・プログラムごとに別々のウィンドウがオープンされる。とりわけ、ウィンドウ・システムは、あるプログラムが作成したある文書から別の無関係のプログラムが作成した別の文書へのデータ転送を容易にするためのいくつかのツールをユーザに提供する。このようなツールの1つは、あるウィンドウでデータを囲み、それを別のウィンドウに移動して挿入する、いわゆる「カット・アンド・ペースト」操作である。この操作は通常、マウスで制御したカーソルを使用して実施される。現在使用されているウィンドウ環境の1つは、AT&T Bell Laboratories社が開発したUNIXオペレーティング・システム（UNIXはNovell社の商標である）上で動作する「Xウィンドウ・システム」（Massachusetts Institute of Technologyの商標）である。

【0003】安全保護ラベルは、Defence Intelligence Agency (DIA) の"Requirements for System High and Compartmented Mode Workstations" (CMW規定という) の基本要件の1つである。この規定では、特に、安全保護が異なる可能性のある複数のウィンドウをいつでもオープンできるような、ワークステーション用の安全なマルチレベル・ウィンドウ・システムを扱っている。このようなウィンドウの安全保護レベルは、安全保護ラベル、すなわち、1つの主題またはオブジェクトに関する全体的な機密レベルを示す必須アクセス管理 (MAC) ラベルと、データの集合体にラベルを付ける情報ラベルという、より細分性の高いラベルとによって管理される。機密レベルまたはMACレベルは、特権ユーザを除くすべてのユーザ向けの「上位読み取りなし」（より高い機密レベルでのオブジェクトの読み取りなし）規則および「下位書き込みなし」（より低い機密レベルでのオブジェクトの書き込みなし）規則で実施される。この「上位読み取りなし」規則のため、通常のユーザはできるだけ高い

機密レベルで作業する傾向があり、そのため、何でもみられるようになっている。しかし、「下位書き込みなし」規則では、その内容がどんなにつまらないものでもすべてのオブジェクトに同一の高い機密レベルでラベルを付けなければならない。このようなデータの過剰分類を防止するため、CMWは、データの「真」の機密性をある程度示す、情報ラベルのシステムを提供している。情報ラベルはユーザ制御とシステム制御の両方があり、ユーザは最初に情報ラベルを設定し、必要に応じて変更することができ、システムは伝播または浮動によりそれを更新する。すなわち、プロセスが機密データを読み取ると、それ自体の（プロセス）情報ラベルがそれが読み取ったすべてのデータの情報ラベルの最大値（最小上限）まで浮動し、その後それが他のオブジェクトに書き込むときには、そのオブジェクトがデータを受け取ることができると想定して、そのオブジェクトの情報ラベルが同様に浮動する。

【0004】機密ラベルと情報ラベルの機密レベルが異なるときにデータのウィンドウ間移動を行うことは、CMWを有用にする基本的特徴の1つである。しかし、すべてのウィンドウ間移動は、前述の「上位読み取りなし、下位書き込みなし」の規則に適合しなければならない。具体的には、カット・アンド・ペースト操作によるラベルの機密レベル変更は、次のように行うことができる。MACラベルの上位移行はすべての特権ユーザと通常ユーザが行うことができ、MACラベルの下位移行は特権ユーザのみ行うことができ、情報ラベルの上位移行または下位移行はすべての特権ユーザと通常ユーザが行うことができる。CMWでは、ユーザがすべてのラベル変更を認識するように、これを対話式に行うよう要求している。

【0005】Xウィンドウ・システムは、1台のXサーバと、様々な機能を実行する複数のアプリケーション・プログラムから構成される。Xサーバは、ユーザ入力の結果として生成される事象の送信により、このようなアプリケーションとやりとりする。Xウィンドウ・システムでは、Xサーバは、Xtermなどの通常は未承認のクライアント・プログラムによって開始され制御される、カット・アンド・ペースト操作を仲介するだけである。カット・アンド・ペースト操作に直接かかわるもう1つのアプリケーションは、ウィンドウ・マネージャである。ウィンドウ・マネージャは、ウィンドウの視覚的操作のほとんどを担当する。

【0006】SecureWareは、ベースとしてXウィンドウ・システムを使用する市販のCMWを備えているが、カット・アンド・ペースト操作には個別のクライアントではなくウィンドウ・マネージャを使用する。SecureWareのインプリメンテーションでは、所与のデータ・タイプしか扱うことができず、クライアントは、承認後のデータの変更や承認前のデータの受信を行なう可能性が

ある。専用の文書以外には、その作業を詳述した文書が発行されておらず、特に、カット・アンド・ペースト操作に関する処理方法については何も発行されていない。Smith他は"Secure Multi-Level Windowing in a B1 Certifiable Secure UNIX Operating System" (Winter 1989 USENIX Conference Proceedings)において、ウインドウ上でのカット・アンド・ペースト操作について記述しているが、この研究はXウインドウ・システムに基づくものではなく、単にMAC準拠に関連しているだけである。情報ラベルの概念はまったく示されていない。Carson他は"From B2 to CMW:Building a Compartmented Mode Workstation on a Secure Xenix Base" (Proceedings of the AIAA/ASIS/IEEE Third Aerospace Computer Security Conference, 1987)において、CMWインプリメンテーションの1つについて記述しているが、このインプリメンテーションでは、そのオペレーティング・システムとしてXENIXを、そのベース・ウインドウ・システムとしてViewnixを使用し、カット・アンド・ペースト操作では完全に中央制御下にあるまったく異なる機構を使用している。(XENIXはマイクロソフト社の商標であり、ViewnixはFive Paces Software社の商標である。)

#### 【0007】

【発明が解決しようとする課題】したがって、本発明の目的は、未承認ウインドウ・システム・クライアント・プログラムが選択マネージャという特殊な承認クライアント・プログラムによって仲介された転送によってユーザーの制御下でユーザーの示唆により安全保護領域間でデータを転送できるようにするための安全な手段を提供することにある。

#### 【0008】

【課題を解決するための手段】本発明により、機密レベル変更カット・アンド・ペースト操作に関するコンパートメント化モード・ワークステーション(CMW)要件の機能を満たすように構成可能な機構が提供される。この機構は、基礎となるオペレーティング・システムが何であってもそのオペレーティング・システムで使用することができる。CMWのカット・アンド・ペースト要件を満たし、機密レベル変更選択機構が抜け道として機能するのを防止するため、本発明の機密レベル変更選択機構の解決策は以下の特徴を有する。

- ・Xサーバは、MAC上位移行操作中の低レベル・プロセスへの通信にダミー・ウインドウIDを使用する。
- ・すべての機密レベル変更操作について、選択が転送される前にXサーバは、転送の続行を許可する前にユーザー確認を要求するポップアップを表示するよう選択マネージャに指示する事象を選択マネージャに送信する。この選択機構は、カット・アンド・ペースト用の構成可能な機密レベル変更選択操作をサポートする(MAC上位移行はすべてのユーザが対象、MAC下位移行は特権ユー

ザが対象、情報ラベルの上位移行と下位移行はすべてのユーザが対象)。Xウインドウの選択は仲介された双方向通信を伴うので、それが「抜け道」として使用されるのを防止するため(また、CMWのカット・アンド・ペースト要件を満たすため)に、安全な選択機構によって以下の特徴も提供される。

1. 選択マネージャは、選択項目所有者の安全保護属性を継承する特殊なウインドウとプロパティを作成し、これを選択項目所有者が使用できるようにする。このため、選択の要求側によって指定されたウインドウIDとプロパティIDは選択項目所有者から隠される。これは、MAC上位移行時に要求側が低レベル・プロセスと通信するときに選択の所有者が要求側に関する安全保護関連情報を入手できないよう行われる。
  - 1 a. 選択項目所有者は、通常のX機構により選択マネージャに選択項目データを転送する。選択マネージャは、データの所有者になり、転送が完了するまでそれにに対する排他的権利を有する。
2. 選択項目所有者から選択項目要求側に転送されるデータをログイン・ユーザが確認できるようにするユーザ・インターフェースが提供される。これにより、ユーザはいつでも増分転送を取り消すことができ、機密レベル変更操作の場合にはデータ転送の続行が許可される前にユーザ確認が要求される。
  - 2 a. ユーザが転送を確認すると、選択マネージャはデータを要求側に転送する。もう1つのコピーを作成する必要性を回避するため、「所定の場所で」転送を行うために新しいプロトコル要求が使用される。
3. 特権の使用を伴う操作(MAC下位移行など)を試みる場合、ならびにデータ転送、再分類、特権の使用を伴う安全保護違反を犯した場合には、適切な監査事象が生成される。
4. 適切に構成されている場合、選択機構は、要求側のウインドウおよびプロパティに関する任意アクセス制御(DAC)書き込みアクセス制限を無効にするための十分な特権を有する。本発明による機構では、すべてのアプリケーションが機密レベル変更選択バッファに書き込みアクセスすることができる。選択バッファに書き込まれるデータは、選択より高レベルにすることことができ、それにより、情報ラベルが浮動し、LabelChange事象という新しい事象が生成される。選択項目に書き込むと、書き込みプロセスがその選択バッファの「所有者」になり、選択バッファが所有者のラベルを継承する。特定の選択項目の保有者が誰であるかの確認を別のアプリケーションが必要とする場合は、情報を要求したアプリケーションより選択項目の現在の保有者の方が機密レベルが高ければ、何も返されない。これにより、選択項目所有権パターンによって情報の抜け道が間接的に防止される。選択バッファ内のデータをコピーできるかどうかは、保有者のアクセス特権によって決まる。情報を要求したアプリ

ケーションに特権が与えられていない限り、そのアプリケーションより選択バッファの方が機密レベルが高ければ、アプリケーションは選択項目内のデータを読み取ることができない。

【0009】上記およびその他の目的、態様、利点は、添付図面を参照しながら本発明の好ましい実施例に関する以下の詳細な説明を読めば、よりよく理解できるであろう。

#### 【0010】

【発明の実施の形態】Xウィンドウ・システムの環境で本発明の好ましい実施例について説明するが、本発明は他のウィンドウ環境でも実施可能であることに留意されたい。すべての機密レベル変更カット・アンド・ペースト操作に対し、Xサーバと、選択マネージャという本発明による新しいクライアントを使用する。

【0011】ここで添付図面、特に図1を参照すると、同図には本発明の好ましい実施例による設計済みCMW用の安全なXウィンドウ・システムの構造が示され、新しい承認クライアントの1つとして選択マネージャ100が示されている。より具体的には、通常、Xウィンドウ・システムは、ローカル・エリア・ネットワーク(LAN)などの通信媒体103により接続された複数のXサーバ101および102を含む。それぞれのXサーバには、ユーザがウィンドウ・システムと対話するためのディスプレイ104、キーボード105、マウス106が備えられている。通信媒体103には、本発明による新しい承認クライアント・プログラムである選択マネージャ100を含む、様々なアプリケーションおよび管理プログラムが接続されている。他の管理プログラムとしては、監査マネージャ107、プロセス・マネージャ108、MWMウィンドウ・マネージャ109、XDMディスプレイ・マネージャ110などがある。Xアプリケーション111の他に、擬似端末装置として機能し、接続されたAIXterm端末アダプタ114を介して通信媒体103と通信するマルチレベル・アプリケーション112と通常アプリケーション113が存在する場合もある。Xサーバ101または102は、ユーザが使用しているものと同じワークステーション上で動作しなければならない。クライアントはこのマシン上にある場合もあれば、他のマシン上にある場合もある。(通常、ウィンドウ・マネージャ109や選択マネージャ100のような「特殊」クライアントは、同一マシン上でローカルに動作するが、これは必須ではない。)

【0012】選択項目はXウィンドウの資源である。選択項目により、アプリケーションは任意のタイプのデータを交換することができ、交換するデータのタイプを折衝することができる。クライアント間通信規則マニュアル(ICC-CM)によれば、選択はクライアント間のカット・アンド・ペースト操作に適した方法である。したがって、本発明による解決策では、機密レベル変更カッ

ト・アンド・ペースト操作のベースとして選択資源を使用する。この手法はX選択資源の現在の使い方と整合するものである。というのは、この手法ではX選択資源自身を変更するわけではないが、安全保護ラベルの機密レベル変更のためのデータ転送に現在使用されているステップ間に追加ステップを挿入するからである。このため、この解決策は、既存の選択資源の当然の拡張として機能する。

【0013】X選択資源の目的は、複数のアプリケーションが情報を共用できるようにすることである。各選択項目は、一度に1人の「所有者」すなわちトークンの保有者しか持てないため、その所有者はカットまたはペースト操作を実行することができる。1つのアプリケーションがカットを行い、別のアプリケーションがペーストを行う場合は、両方のアプリケーションが先在するX選択要求事象により互いにやりとりする。ワークステーションにとってグローバルな選択項目の数はいくつでもよい。それぞれの選択項目は、アトムによって命名され、クライアントによって所有され、ウィンドウに接続される。

【0014】機密レベル変更選択機構の目的は、適切なMACラベルおよび情報ラベルをペースとするデータに関連づけることである。これは、ポップアップの使用により対話式に、または選択マネージャの構成資源ファイルの構成オプションの設定により非対話式に行うことができる。いずれの場合でも、データのラベル変更に関する標準方針は変わらない。すなわち、MACラベルの上位移行はすべての特権ユーザと通常ユーザに許可され、MACラベルの下位移行は特権ユーザだけに許可され、情報ラベルの上位移行または下位移行はすべての特権ユーザと通常ユーザに許可される。(実際に使用する方針もシステム管理者によって構成可能である。)ユーザがすべてのラベル変更を認識するように、CMWの要件の1つである対話式で機密レベル変更を行う方法について以下に説明する。

【0015】図2は、非増分カット・アンド・ペーストを示している。これは、データ転送が1回だけ行われること、すなわち、すべてのデータが同時に転送されることを意味する。図2のアスタリスク\*は、選択マネージャがXSendEventを使用してこの事象を送信し、他のすべての事象はXサーバによって送信されることを意味する。増分転送では、所与の時点でデータの一部分だけが転送され、1回の転送ごとに所与の検査を行わなければならない。まず図2を参照して非増分ケースについて説明し、次に図3を参照して増分カット・アンド・ペースト操作について説明する。ただし、図2および図3にXサーバが示されていなくても、このプロセスにはXサーバがかかわる(Xサーバによって送信される事象のうち、後ろにアスタリスクが付いていない事象のすべて)ことに留意されたい。また、構成可能なオプションがす

べて設定されているものとして説明を進めることにも留意されたい。たとえば、システム管理者がそのオプションを禁止した場合には、以下に説明するポップアップ・メニューが表示されない場合がある。

【0016】図2は、単純な（非増分）選択に関する選択要求を要求するための修正済みプロトコル内の選択項目要求側と選択項目所有者との間のプロトコルを示している。第1のステップでは、要求側がXConvertSelectionプロトコル要求を出し、それをXサーバがSelectionRequestLabelプロトコル要求に変換し、SelectionRequestLabel事象として選択マネージャに転送する。選択マネージャは、図のステップ2に示すようにMACダイアログとDACダイアログを表示する。ステップ3では、選択マネージャが専用のウィンドウ上でプロパティを作成し、選択項目の所有者は後でそのウィンドウ上でその選択項目をポストすることができる。次に選択マネージャはステップ4でSelectionRequestを生成し、これを最初に意図した受信側に送信する。これは標準のSelectionRequest事象なので、この環境で機能するように受信側のコードを変更する必要はない。

【0017】選択マネージャは、この事象でそれ自体のプロパティを示す。この事象に応答して、選択項目所有者がステップ5で選択マネージャのプロパティで選択項目データをポストし、ステップ6で選択マネージャに対してSelectionNotify事象を出す。次に選択マネージャは、ステップ7で選択項目所有者から選択項目要求側に渡されるデータをユーザが検査できるようにする。これにより、ユーザは、未修正の通過の要求を許可するか、要求を取り消すか、または転送中のデータを下位移行できるようになる。要求を取り消すと、ステップ8で監査事象を生成することができる。この場合、選択マネージャは続行する前に監査レコードが書き出されるのを待つ。これは、ダイアログのステップ9に示されている。ステップ10では、選択マネージャが新しいXTransferProperty呼出しを使用して、それ自体のウィンドウ/プロパティから選択項目要求側のウィンドウ/プロパティに選択項目データを転送する。次に選択マネージャはステップ11でSelectionNotify呼出しを出し、その結果、元のXConvertSelection呼出しに指定されたプロパティでその選択項目が使用可能かどうかが要求側に通知される。ステップ12では、要求側がそのデータを読み取り、次にステップ13でXPropertyNotify呼出しを出し、その結果、選択マネージャに事象が送信される。選択マネージャはステップ14でそれ自体のデータ構造を終結し、ステップ15でプロパティ通知を所有者に転送する。したがって、所有者は、この時点で必要とするすべての終結処置を実行することができる。これで、図2に示すハンドシェークにかかわるすべてのステップの説明を完了する。

【0018】図3は、増分選択項目が転送されていると

きに行われるハンドシェーク・プロトコルを示している。増分選択項目は、1つの選択項目としてではなく、複数の部分に分けて転送することに意味があるほど、大きいものである。このプロトコルは、要求側がまずそれ自体のウィンドウでダミー・プロパティを出すことから始まる。要求側はXConvertSelectionプロトコル要求を出し、それをXサーバがSelectionRequestLabelプロトコル要求に変換し、SelectionRequestLabel事象として選択マネージャに転送する。ステップ2では、非増分ケースのように選択マネージャがMACダイアログとDACダイアログを表示する。ステップ3では、選択マネージャは、選択項目の所有者が後でその選択項目をポストすることができる専用のウィンドウ上でプロパティを作成し、MACダイアログとDACダイアログを表示する。次に選択マネージャは、ステップ4で選択項目所有者に要求を転送する。ステップ5では、選択項目所有者（これが増分選択項目であることを認識している所有者）が選択マネージャのウィンドウ上でそのプロパティをポストし、次にステップ6で、これが増分（INC R）選択項目であることを選択マネージャに通知するSelectionNotifyを出す。したがって、選択マネージャは、そのデータが複数の部分に分かれて到着する（可能性がある）ことを認識する。次に選択マネージャは、ステップ7で選択項目所有者から選択項目要求側に増分式に渡されるデータをユーザが検査できるようにする。要求を取り消すと、ステップ8で監査事象を生成することができる。ステップ9では、選択マネージャが新しいXTransferProperty呼出しを使用して、それ自体のウィンドウ/プロパティから選択項目要求側のウィンドウ/プロパティに選択項目データを転送する。次に選択マネージャは、ステップ10でSelectionNotify（INC R）呼出しを出す。したがって、要求側は、そのデータが複数の部分に分かれて到着する可能性があることを認識する。実際のデータ転送は、ステップ11～14で一連のChangePropertyメッセージとPropertyNotifyメッセージを使って行われる。選択マネージャは、データのレベルを検査して変更し、いつでも選択項目を取り消すことができる機会をユーザに与える。選択マネージャは、1回の転送分としてそれぞれの部分を転送する。唯一の違いは、要求側が個別のXconvertselection要求を送信するのではなく、要求側が転送されたデータを読み取って削除することによって、その後の転送が通知される点である。

【0019】このプロトコルの最後のステップは、ステップ13に示すように、プロパティ所有者が選択マネージャのプロパティで長さがゼロのプロパティ（ダミー）をポストすることである。これにより、転送が完了したことが通知され、それに応答して選択マネージャがステップ14でこの情報を選択項目要求側に転送する。これで選択項目要求側は転送が完了したことと、ステップ1

5～17の单一転送ケースのようにハウスキーピング・プロシージャを認識することになる。

【0020】このプロセスについては、図4の流れ図に示す。データ転送を行うためには、データ所有者は選択資源所有者にならなければならない。選択アトムは公用資源なので、どのクライアントも選択項目所有権を確認することができる。クライアントがこのデータの受取りを必要とする場合、そのクライアントはデータの所有者にXConvertSelection要求を送る。このXconvertselection要求を受け取ると、Xサーバは、要求を行ったクライアントがその宛先として指定している要求側のウィンドウとプロパティに対して正しいアクセス権を持っていることを確認する。正しいアクセス権を持っている場合には、Xサーバは、SelectionRequestLabel事象という新しい事象としてこのSelectionRequest事象を選択マネージャに転送する。この事象は、選択項目所有者のMAC、ユーザID (UID)、グループID (GID)と、要求側のウィンドウおよびプロパティに関するMACラベルおよびDAC属性とを含んでいる。この事象を受け取る際の選択マネージャの挙動は構成可能である

(すなわち、システム管理者の資源ファイル内の使用に依存する)が、デフォルト挙動では、同じMACレベルの要求がMACアクセス検査に合格する(そして監査を受けない)。

【0021】特に図4を参照すると、まず判断ブロック401では、要求側のMAC (Rmac) が所有者のMAC (Omac) より大きいか、等しいか、小さいかを判定するためにテストが行われる。要求側が所有者とは異なるMACレベルにある場合、選択マネージャは、判断ブロック402でそのユーザーが特権下位移行者であるかどうかを確認し、判断ブロック403で上位移行が許可されているかどうかを確認する。いずれの場合にも、選択マネージャはまず、ユーザ・ログイン時にディスプレイ・マネージャ (xdm) によってルート・ウィンドウ・プロパティとしてポストされたユーザおよびグループ・リストを入手する。次に、下位移行特権の有無を検査するために、選択マネージャは、それ自体を承認プロセスとして指定し、下位移行特権の有無を検査することと、パラメータとしてユーザID (UID) およびグループID (GID) とを指定して、AIXのtcl(承認プロセス制御リスト)機能呼出し(他のオペレーティング・システムの場合は、同様の機能を持つシステム呼出し)を行う。(AIXはIBMの商標であり、UNIXオペレーティング・システムのIBM版である。)

【0022】判断ブロック402でユーザーが特権下位移行者であるかどうかを判定するテストを行うケースを考慮すると、ユーザーが特権下位移行者ではないと判定された場合、その結果、機能ブロック404に示すように、要求失敗が発生する。すると、図5に示すポップアップが表示され、機能ブロック405で要求側に失敗事象が

送られ、システムへの復帰が行われる前に機能ブロック406で選択マネージャが監査事象を生成する。これに對して、ユーザーが特権下位移行者である場合は、図6に示すポップアップが表示され、ユーザーに下位移行確認を要求する。判断ブロック407で判定されたように、ユーザーがポップアップから「取消し」を選択した場合は、図5に示すポップアップが表示され、機能ブロック405で要求側に失敗事象が送られ、システムへの復帰が行われる前に機能ブロック406で選択マネージャが監査事象を生成する。ユーザーが図6に示すポップアップから「OK」を選択した場合は、機能ブロック408で監査事象が生成される。というのは、下位移行はユーザーのための許可の用途の1つであるからである。

【0023】判断ブロック403で上位移行が許可されているかどうかを判定するテストを行うケースを考慮すると、上位移行が許可されていないと判定された場合、その結果、図6に示すポップアップが表示される。これは、MAC上位移行警告である。ユーザーが「取消し」を選択した場合は、図5に示すポップアップが表示され、機能ブロック409で要求側に失敗事象が送られ、システムへの復帰が行われる前に機能ブロック410で選択マネージャが監査事象を生成する。これに對して、ユーザーが図6に示すポップアップで「OK」を選択したか、判断ブロック401で判定されたように要求側ウィンドウMACと所有者プロセスMACが等しい場合には、判断ブロック411で書き込みアクセスが要求されたかどうかを判定するテストが行われる。書き込みアクセスが要求されていない場合は、図7に示すポップアップが表示され、転送を続行すべきかどうか示すようユーザーに要求する。判断ブロック412で判定されたように、ユーザーが図7のポップアップで「取消し」を選択した場合は、図8に示すポップアップが表示される。次に機能ブロック405で要求側に失敗事象が送られ、システムへの復帰が行われる前に機能ブロック406で選択マネージャが監査事象を生成する。ユーザーが図7に示すポップアップで「OK」を選択したか、判断ブロック411で判定されたように書き込みアクセスが要求された場合には、機能ブロック413で所有者がプロパティを書き込む。機能ブロック414では、さらにデータが修正されるのを防止するため、選択マネージャがプロパティの所有権を自分自身に変更する。次に機能ブロック415では、図9に示すポップアップが表示され、要求されたデータに関するラベル情報を提供するよう要求側に要求する。

【0024】この時点では、これが増分(INCR)転送であるかを判定するテストが判断ブロック416で行われる。増分転送である場合には、次に、これが増分転送の最初の部分であるかどうかを判定するテストが判断ブロック417で行われる。最初の部分である場合には、図10に示すポップアップが表示され、1回のデータ転送ごとに情報ラベルを求めるプロンプトが必要かどうか

を示すよう、要求側に要求する。図10のポップアップから要求側が何を選択しても、図3に関連して記載したプロトコルに従って、機能ブロック418で最初にヘッダが要求側に転送され、機能ブロック419で選択項目データの残りの部分が所有者から増分式に獲得され、プロセスはループをたどって機能ブロック414に戻る。毎回情報ラベルを要求することを要求側が選択した場合には、1回のデータ転送ごとに図11に示すポップアップが表示され、要求側に情報ラベルを要求する。増分転送ではないか、増分転送の最初の部分以降ではない場合には、図12に示すウィンドウが表示され、図2および図3に関連して記載したプロトコルに従って、機能ブロック419でシャドー・ウィンドウから要求側ウィンドウにプロパティが転送される。

【0025】簡単に要約すると、下位移行または上位移行カット・アンド・ペースト操作の許可がユーザに与えられていない場合、選択マネージャは、図5に示す警報ボックスを表示し、拒否を示す監査事象を作成し、プロパティなしを指定したSelectionNotify事象を要求側に戻し、選択プロセスを終了する。MAC検査が成功した場合は、選択マネージャはDACアクセス検査を実行する。要求側ウィンドウ/プロパティが所有者に書き込みアクセスを許可していない場合は、図7に示すDACダイアログ・ポップアップにより、そのユーザが要求側のウィンドウまたはプロパティへの書き込みアクセスを所有者プロセスに許諾する必要があるかどうかの質問が行われる。ユーザが肯定の応答を行うと、これは、ウィンドウ/プロパティへの要求側の書き込みアクセスを所有者に与える効果を持ち、特権の使用に関する監査事象（ただし、選択マネージャはDAC免除者である）が生成される。ユーザはMAC問題が一切発生しないときにカット・アンド・ペースト操作の実行が許可されるので、これは、アクセス制御リスト（ACL）とは無関係にペースト操作をサポートするすべてのウィンドウについて許可される。システムがDACを迂回するように構成されていない場合は、図8に示す警告が表示され、選択が失敗に終わり、監査事象が生成される。上記のMAC検査とDAC検査が成功すると、選択マネージャは、カット・アンド・ペースト操作に使用する「シャドー」ウィンドウと「シャドー」プロパティを作成する。この新しいウィンドウとプロパティには、所有者のMACレベルなど、選択項目所有者の安全保護属性が与えられる。これにより、選択項目所有者は選択項目データを安全に書き出せるようになる。（選択マネージャには特権が与えられているので、このウィンドウとプロパティにいつでもアクセスすることができる。）この「シャドー」ウィンドウIDと「シャドー」プロパティIDは、選択項目所有者に送られる後続のすべての事象の際に、要求側のウィンドウIDとプロパティIDの代わりに使用される。このため、要求側のウィンドウIDとプロパティIDが

所有者から隠され、所有者は別のMACレベルにあると思われるウィンドウおよびプロパティのIDを確認できなくなる。その場合、選択マネージャは、データ所有者に送るSelectionRequest事象を作成する際に要求側のIDの代わりにこれらのIDを挿入する。また、選択マネージャは、要求側のウィンドウ上でPropertyNotify事象の送信請求も行うので、データ所有者へのこれらの事象の送信を仲裁し、「シャドー」ウィンドウIDと「シャドー」プロパティIDを挿入することができる。

【0026】所有者がSelectionRequest事象を受け取ると、データ所有者は、XchangeProperty呼出しを使用することにより、「シャドー」プロパティ上にデータをポストする。次に選択項目所有者は、「シャドー」ウィンドウIDと「シャドー」プロパティIDとを使用して、そのデータがプロパティにポストされたことを要求側に示すSelectionNotify事象を要求側に送信する。このSelectionNotify事象はXサーバによって仲裁され、Xサーバはそれに代わって新たに定義されたSelectionLabel事象を選択マネージャに送る。その事象は、要求側クライアントおよび要求側のウィンドウの情報ラベルと、所有者クライアントの情報ラベルとを含む。（これは、選択マネージャによる追加照会の必要性をなくすために行われる。）SelectionLabel事象を受け取ると、選択マネージャはまず、そのデータの所有権を自分自身に変更する。これにより、選択マネージャによる偶発的または作成的なデータの変更が防止される。特に、これにより、黙認している選択項目所有者がユーザ承認のために無害のデータを提示し、承認後（ただし、データが実際に要求側に転送される前）に機密データを密かに挿入することが防止される。選択マネージャは、選択マネージャのシステム管理資源ファイルで選択された構成オプションに応じて、選択項目データの情報ラベルを宛先のウィンドウの情報ラベルあるいは入力情報ラベルまたは要求側クライアントの情報ラベルのいずれかと比較する。情報ラベルを要求するよう構成されている場合、選択マネージャは、図10に示すダイアログ・ボックスを表示し、そのデータの情報ラベルをユーザに要求する。

【0027】上記のように、このダイアログ・ボックスにより、ユーザは選択項目のラベル情報を希望通りに変更することができる。OKを選択した場合は、その選択項目のラベルが変更され（必要な場合）、監査事象が作成される。取消しを選択した場合は、（ICCCM通りに）選択項目が削除され、プロパティなしを指定したSelectionNotify事象が要求側に送られる。取得オプションは、対応する表示ウィンドウ・ラベルを選択項目ラベル（さらに編集される可能性がある）にコピーする。ユーザが無効なラベルを入力すると、エラー・ポップアップのメッセージ域に"Invalid label please re-enter"というメッセージが表示され、監査事象が生成され、ユーザはラベルを再入力する機会を得る。このメッセージ

は、そのデータについて入力された情報ラベルが要求側のプロパティのMACレベルより高い場合にも表示される（この場合にも監査事象が生成される）。ユーザは、そのデータに関する情報ラベルを選択する前にデータを表示する機会も与えられる。（選択マネージャは、テキスト、ビットマップ、ピクセルマップ、整数という「標準」形式をサポートしている。他のタイプのサポートは、タイプ固有のハンドラを組み込むことによって追加することができる。未知のデータ・タイプはいずれも16進ダンプとして表示される。）データを表示する場合、選択マネージャは、プロパティから「シャドー」ウィンドウにデータを移し、それを図12に示すウィンドウに表示する。

【0028】情報ラベル変更サブウィンドウをクリックすると、ユーザは、データを表示している間に対話式に選択項目データにラベルを付けることができる。ユーザに対して情報ラベルが一切要求されない場合（すなわち、情報ラベルの要求を禁止するようにシステム管理者が資源ファイルでそのオプションを構成してある場合）には、情報ラベルが異なっていても（すなわち、選択項目データのラベルがデフォルトで選択されても）選択が続行するが、この違いを示す監査事象が生成される。

【0029】監査マネージャは、その初期設定プロセスを完了した後、監査マネージャが監査事象を受け入れられる状態になっていることを選択マネージャ、Xサーバ、その他の特権クライアントに伝えるルート・ウィンドウ・プロパティをポストする。選択マネージャは、このルート・ウィンドウ・プロパティの有無を検査した後、新たに定義したAuditNotify事象を使用して監査マネージャに監査情報を送信する。このAuditNotify事象は、事象が生成された理由（たとえば、特権の使用／誤用、データのラベル変更など）を示すものである。また、この事象は、「シャドー」ウィンドウIDと「シャドー」プロパティIDならびにソース・ウィンドウと宛先ウィンドウのウィンドウIDとプロパティIDも含んでいる。前述の図2および図3のステップ8に示すように通常のカット・アンド・ペースト・プロセス（すなわち、違反なし、特権の使用なし）の一部として選択マネージャによってAuditNotify事象が送られる場合は、監査データをポストする必要がない。カット・アンド・ペーストがMACラベルの下位移行を伴っていた場合（すなわち、ユーザが下位移行者特権を有していた場合）は、CMW要件により、選択項目データも監査レコードに含まれていなければならない。したがって、選択マネージャは「シャドー」ウィンドウIDと「シャドー」プロパティIDを監査事象に含める。監査マネージャはこれらを使用して、データのコピー入手し、それを監査証跡に入れる。（データが多すぎて1つの監査レコードで処理できない場合は、元のレコードに次のレコードへのリンクを含める。）次に、選択マネージャは、監査マ

ネージャがAuditNotifyタイプを指定したClientMessage事象を送り返して、監査レコードの作成とその監査証跡バッファへの接続を完了したことを選択マネージャに示すまで待つ。

【0030】監査マネージャからClientMessage事象を受け取った後、選択マネージャは、新たに定義したXTransferPropertyというX1ibの呼出しを呼び出して、「シャドー」プロパティから要求側のウィンドウに関連するプロパティにデータ・ポインタを移動する。その結果、このプロパティは要求側からアクセス可能になる。XTransferProperty呼出しが失敗すると、選択マネージャは、なしというマークを付けたSelectionNotify事象を作成し、これを要求側に送信する。XTransferProperty呼出しが失敗すると、選択マネージャは、要求側のウィンドウIDとプロパティIDとを含むSelectionNotify事象を作成し、これを要求側に送信する。ICCCM要件により、要求側はそのプロパティからデータを読み取って、プロパティを削除し、その結果、PropertyNotify事象が送信される。PropertyNotify事象を受け取ると、選択マネージャは「シャドー」ウィンドウと「シャドー」プロパティを削除する。所有者が「シャドー」ウィンドウ上でPropertyNotify事象を送信請求している場合、所有者は、この事象を受け取ると、選択操作が完了したことを認識する。

【0031】増分カット・アンド・ペーストは、所有者が「シャドー」ウィンドウ上にデータをポストする時点まで、上記の非増分カット・アンド・ペーストと同じように進行する。所有者がデータの増分送信を必要とする場合は、所有者は、SelectionNotify事象にINCRタイプと転送のサイズを含める。次にXサーバはこれをSelectionLabel事象に含める。上記の図9に示すように選択マネージャが第1のセグメントの情報ラベルを要求した後、ユーザは、図10に示すポップアップを使用して増分転送のオプションを選択するよう要求される。

【0032】ユーザは、それぞれの転送ごとに情報ラベル・ダイアログ・ボックス（図11）を表示させるか、それ以上の情報ラベル・ポップアップは表示させないかを選択することができる。要求側にSelectionNotify事象を送信する場合、選択マネージャはタイプINCRと選択項目のデータの長さを含める。必要であれば、すべてのデータが送信されるまで増分転送ごとに監査事象と情報ラベル・ポップアップを生成されて、増分転送が進行する。所有者がデータ転送を実行すると、長さゼロを指定した「シャドー」プロパティに関するPropertyNotify事象が送信される（定義により、データを一切含まないオブジェクトにはシステム・ローという情報ラベルが付いているので、転送されたプロパティの長さがゼロの場合、選択マネージャは情報ラベル・ダイアログ・ボックスを一切表示しない）。要求側のプロパティに関して長さゼロを指定したPropertyNotify事象を受け取ると、

選択マネージャは、データの最後の部分が要求側によって削除されたことを認識する。次に選択マネージャは「シャドー」プロパティと「シャドー」ウィンドウを削除する。所有者は、所有者がこの事象を送信請求していると想定した、「シャドー」プロパティに関して長さゼロのPropertyNotify事象を受け取る。これで増分転送が完了する。

【0033】要求側がXConvertSelectionプロシージャのターゲットとして複数をリストする場合、要求側は、複数のXConvertSelection要求を送信しなければならないわけではなく、一度に複数のプロパティに選択項目を転送するよう所有者に要求している。これは、要求側と所有者が同じMACレベルにある場合のみ許可されるので、Xサーバが複数の要求について偽IDを生成することはない。上記のものとの唯一の変化は、ベースとするデータについて新しい情報ラベルを要求するときに、データが転送されるすべてのプロパティをリストし、そのうちの1つを強調表示したボックスをウィンドウ・マネージャが表示する点である。要求側がボタンを押すと、要求側がそのデータ用の新しい情報レベルを入力できるように、強調表示したプロパティについて図11に示すダイアログ・ボックスが表示される。これは、そのプロパティに関するすべてのデータのラベルが変更されるまで続行される。ただし、複数の要求はすべての同じMACレベルにあるプロパティについてのみ機能し、それぞれのプロパティについてラベルを変更すると監査事象が生成されることに留意されたい。

【0034】1つの好ましい実施例について本発明を説明してきたが、当業者であれば、特許請求の範囲の精神および範囲内で修正を加えた本発明が実施可能であることを理解できるであろう。

【0035】まとめとして、本発明の構成に関して以下の事項を開示する。

【0036】(1) 安全なウィンドウ・システム用の機密レベル変更選択機構において、前記ウィンドウ・システム上の個別のウィンドウで動作し、それぞれがそのウィンドウ内にデータを表示する、複数のクライアント・プログラムと、あるクライアント・プログラム・ウィンドウから別のクライアント・プログラム・ウィンドウにデータを転送するためのカット・アンド・ペースト操作用の選択マネージャというクライアントとを含み、前記選択マネージャがコンパートメント化モード・ワークステーション(CMW)要件を満たし、状態の変化をアプリケーションに通知するためにアプリケーションに事象を送信し、前記選択マネージャが転送中のデータの所有権およびその他の安全保護プロパティを操作して、制御式検査可能データ転送の実行を可能にすることを特徴とする、機密レベル変更選択機構。

(2) 必須アクセス管理(MAC)上位移行操作中の低レベル・プロセスへの通信時に、前記ウィンドウ・シス

テムがダミーのウィンドウIDを使用することを特徴とする、上記(1)に記載の機密レベル変更選択機構。

(3) すべての機密レベル変更操作について、選択項目が転送される前に前記ウィンドウ・システムが前記選択マネージャに事象を送信し、その結果、転送続行が許可される前にユーザ確認を要求するポップアップを選択マネージャが表示することを特徴とする、上記(1)に記載の機密レベル変更選択機構。

10 (4) 安全なウィンドウ・システム内で安全保護属性を有するデータを安全に転送する方法において、データへのアクセスに関する事前定義安全保護レベルを有する要求側からデータ転送に関する要求をウィンドウ・システムが受け取るステップと、要求側によって指定されたウィンドウIDとプロパティIDが選択側所有者から隠されて、要求側が必須アクセス管理(MAC)上位移行時に低レベル・プロセスと通信するときに選択項目の所有者が要求側に関する安全保護関連情報を入手できないようするために、特殊なウィンドウが選択項目所有者からアクセス可能になる、前記ウィンドウ・システム上で動作する選択マネージャというクライアント・プログラムが、選択項目所有者の安全保護属性を継承する特殊なウィンドウとプロパティを作成するステップとを含むことを特徴とする、安全なデータ転送方法。

20 (5) 前記選択項目所有者が前記選択マネージャに選択項目データを転送するステップであって、転送が完了するまで前記選択マネージャがデータの所有者になり、それに対する排他的権利を有するステップと、前記選択項目所有者から選択項目要求側に転送されるデータをログイン・ユーザが検査できるようにし、機密レベル変更操作について、データ転送の続行が許可される前にユーザ確認を要求するユーザ・インターフェースを提供するステップとをさらに含むことを特徴とする、上記(4)に記載の安全なデータ転送方法。

30 (6) MAC下位移行の使用にかかる操作を試みた場合およびデータ転送および再分類にかかる安全保護違反を犯した場合に監査事象を生成するステップをさらに含むことを特徴とする、上記(5)に記載の安全なデータ転送方法。

40 (7) 要求側のウィンドウとプロパティに対する任意アクセス制御(DAC)書き込みアクセス制限を指定変更するため十分な特権を有する選択機構を提供するステップをさらに含むことを特徴とする、上記(6)に記載の安全なデータ転送方法。

(8) 選択項目要求側と選択項目所有者との間で安全なウィンドウ・システム内で安全保護属性を有するデータを安全に転送する方法において、前記選択項目要求側がウィンドウ・システムを動作させる選択マネージャというクライアントに転送される要求を出すステップと、前記選択マネージャが必須アクセス管理(MAC)ダイアログと任意アクセス制御(DAC)ダイアログを表示す

るステップと、後で選択項目の所有者が選択項目をポストすることができる専用のウィンドウ上で前記選択マネージャがプロパティを作成し、選択項目要求を生成し、最初に意図した受信側として前記選択項目所有者に前記選択項目要求を送信するステップと、前記選択項目要求に応答して、前記選択項目所有者が前記選択マネージャのプロパティ上で選択項目データをポストし、前記選択マネージャに選択通知事象を出すステップと、ユーザが未修正通過の要求を許可するか、要求を取り消すか、または転送中のデータを下位移行できるように、前記選択項目所有者から前記選択項目要求側に渡されるデータをユーザが検査できるようにするステップと、ユーザが要求を取り消した場合に監査事象を生成するステップと、前記選択マネージャがそれ自体のウィンドウ/プロパティから前記選択項目要求側のウィンドウ/プロパティに選択項目データを転送し、そのプロパティ上の前記選択項目の可用性に関する通知を要求側に出すステップと、前記選択項目要求側がデータを読み取り、前記選択マネージャに通知を出すステップと、前記選択マネージャがデータ転送の完了を所有者に通知するステップとを含むことを特徴とする、安全なデータ転送方法。

(9) 前記選択マネージャによる前記転送ステップが増分式に実行され、それぞれの転送ごとに個別にラベルを付けるかどうかを指定するようユーザに要求するステップをさらに含むことを特徴とする、上記(8)に記載の安全なデータ転送方法。

【図面の簡単な説明】

【図1】本発明の好ましい実施例によるXウィンドウC MWアーキテクチャを示すブロック図である。

【図2】監査を伴う非増分カット・アンド・ペーストの

プロセスを示すブロック図である。

【図3】監査を伴う増分カット・アンド・ペーストのプロセスを示すブロック図である。

【図4】本発明により実施されるデータ転送プロセスの論理を示す流れ図である。

【図5】コンピュータ画面上に表示されるポップアップ MAC拒否警報ボックスの模写図である。

【図6】上位移行/下位移行の確認のためにコンピュータ画面上に表示されるポップアップ・ダイアログ・ボックスの模写図である。

【図7】コンピュータ画面上に表示されるポップアップ DACアクセス・チェック・ボックスの模写図である。

【図8】コンピュータ画面上に表示されるポップアップ DAC拒否警報ボックスの模写図である。

【図9】コンピュータ画面上に表示されるポップアップ・ラベル・ダイアログ・ボックスの模写図である。

【図10】コンピュータ画面上に表示されるポップアップ増分転送メニューの模写図である。

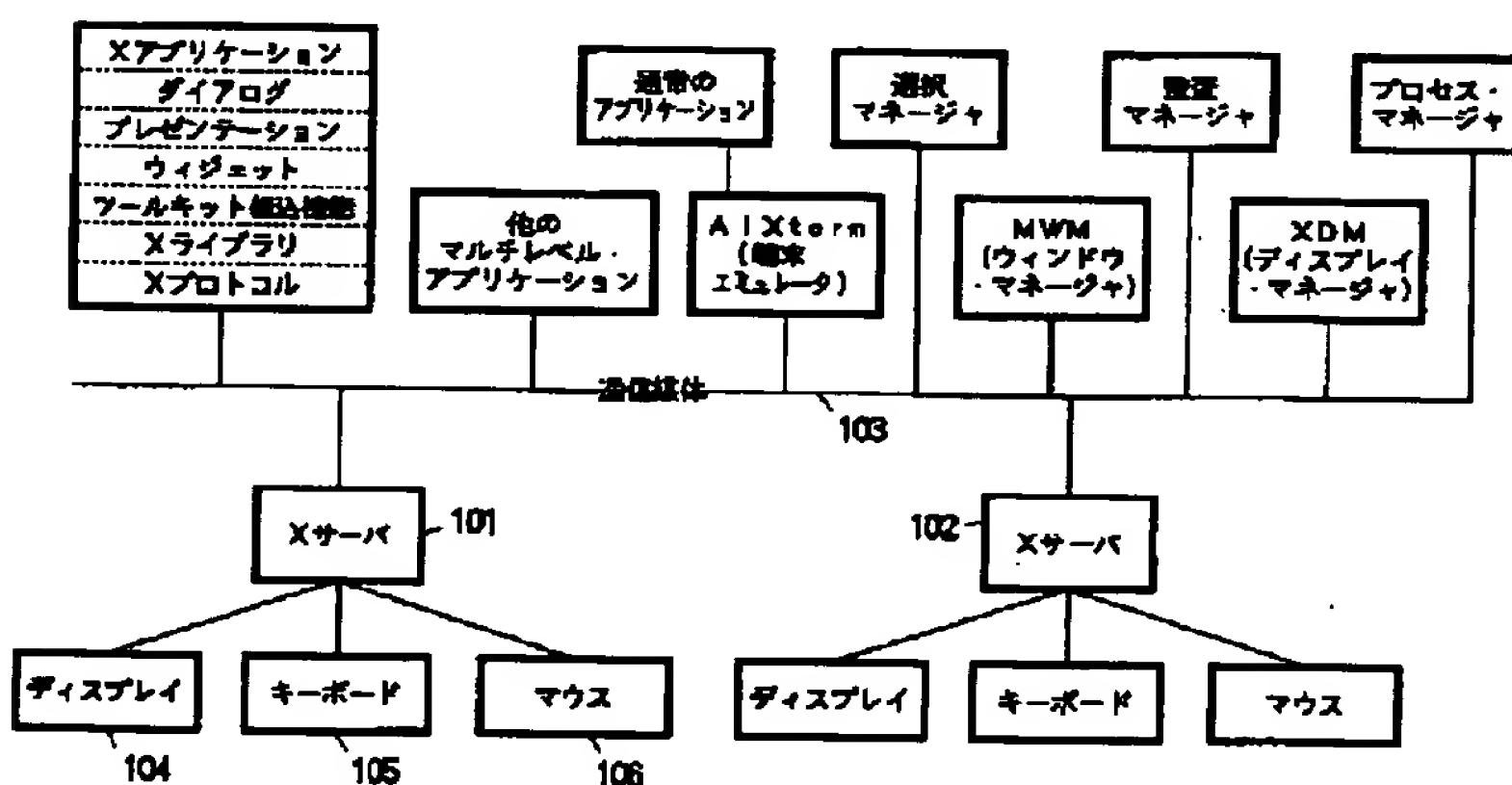
【図11】コンピュータ画面上に表示されるポップアップ選択項目データ・ラベル・ダイアログ・ボックスの模写図である。

【図12】コンピュータ画面上に選択項目データを表示するためのウィンドウ外観の模写図である。

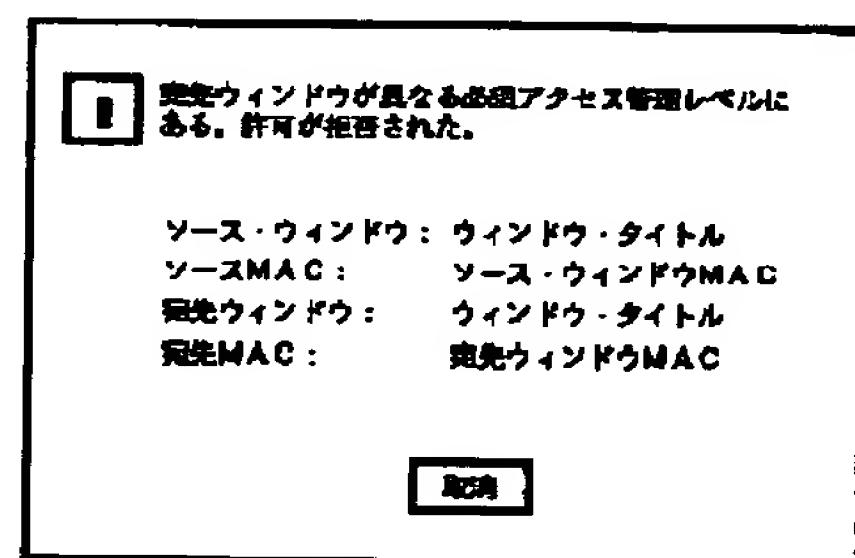
【符号の説明】

- 101 Xサーバ
- 102 Xサーバ
- 103 通信媒体
- 104 ディスプレイ
- 105 キーボード
- 106 マウス

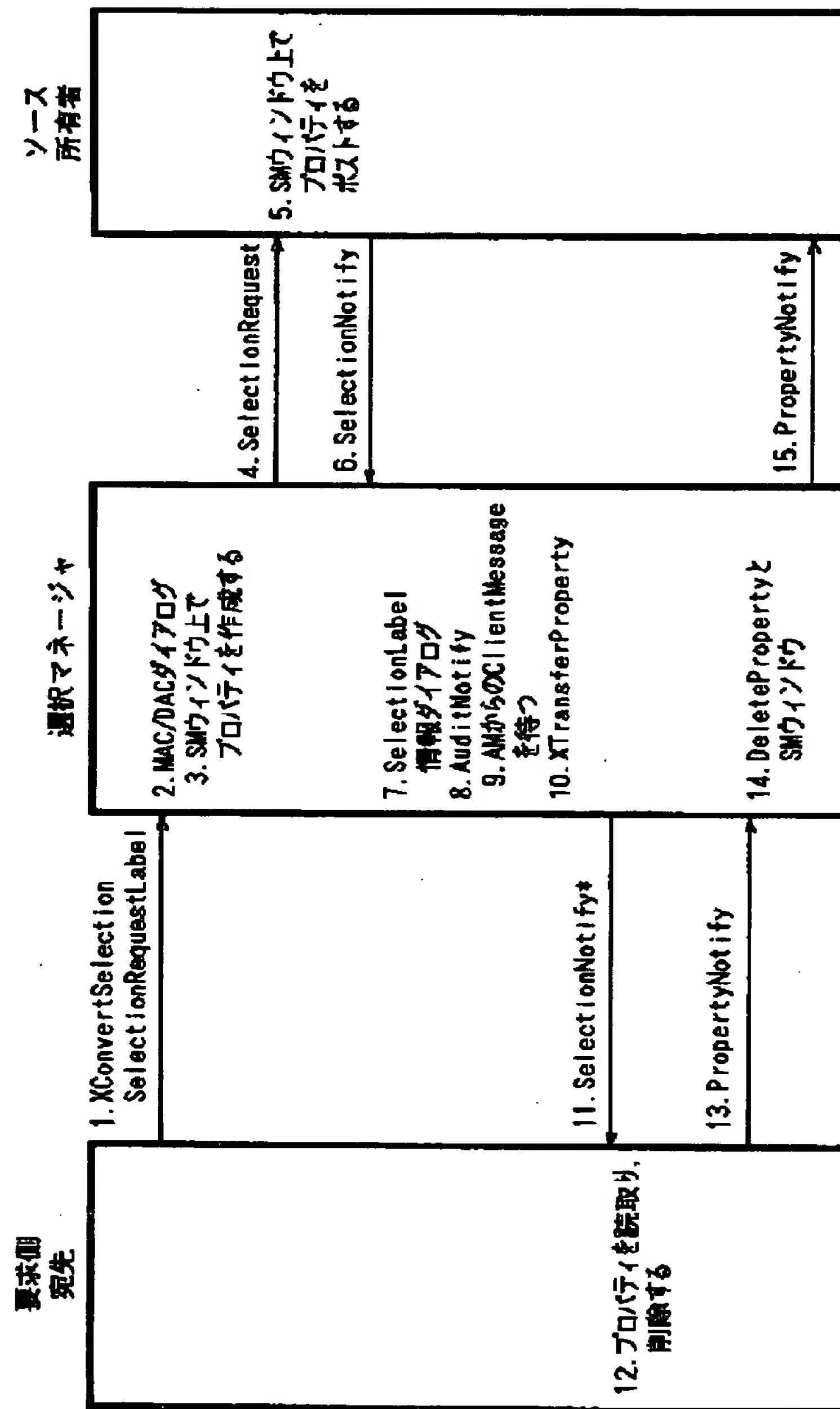
【図1】



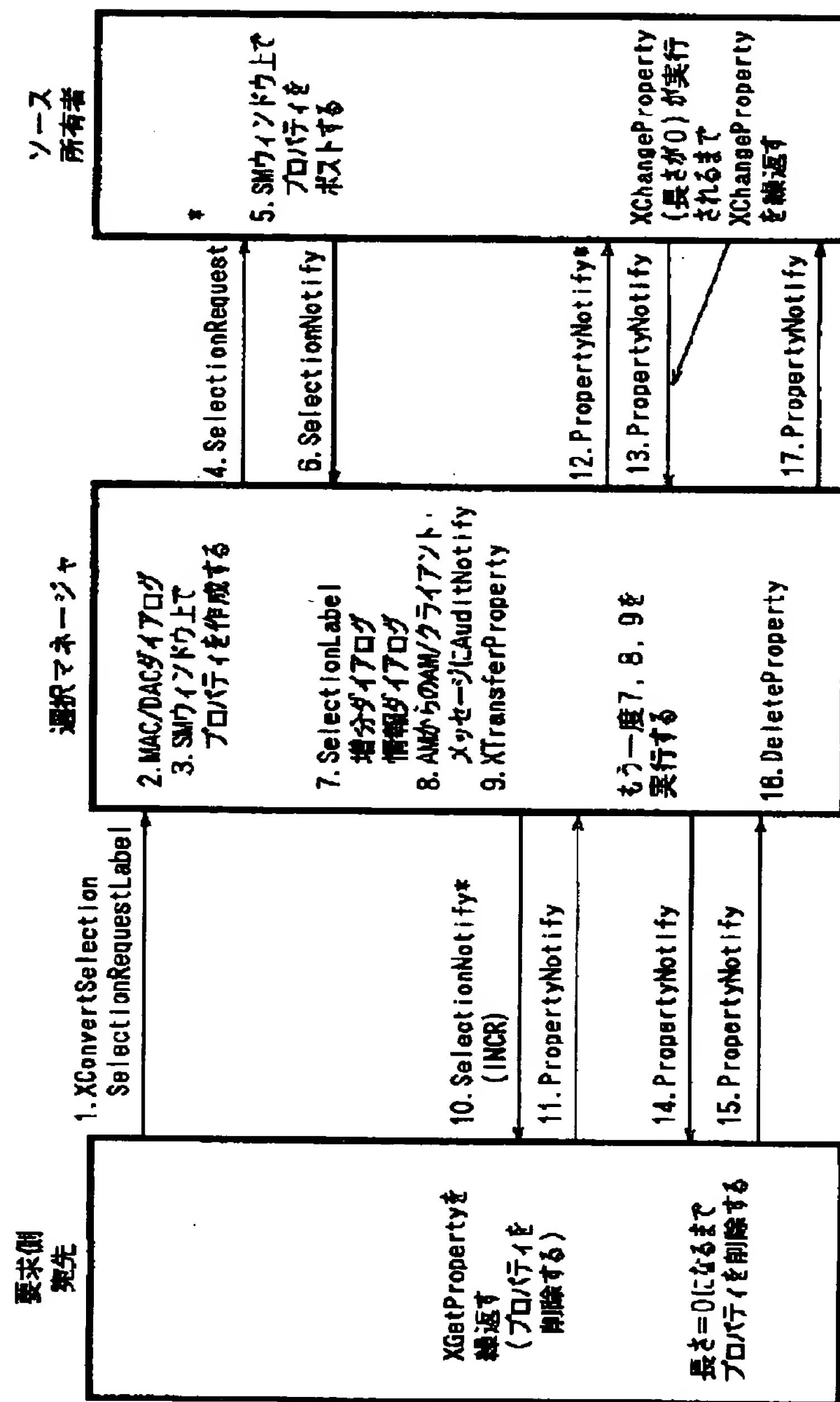
【図5】



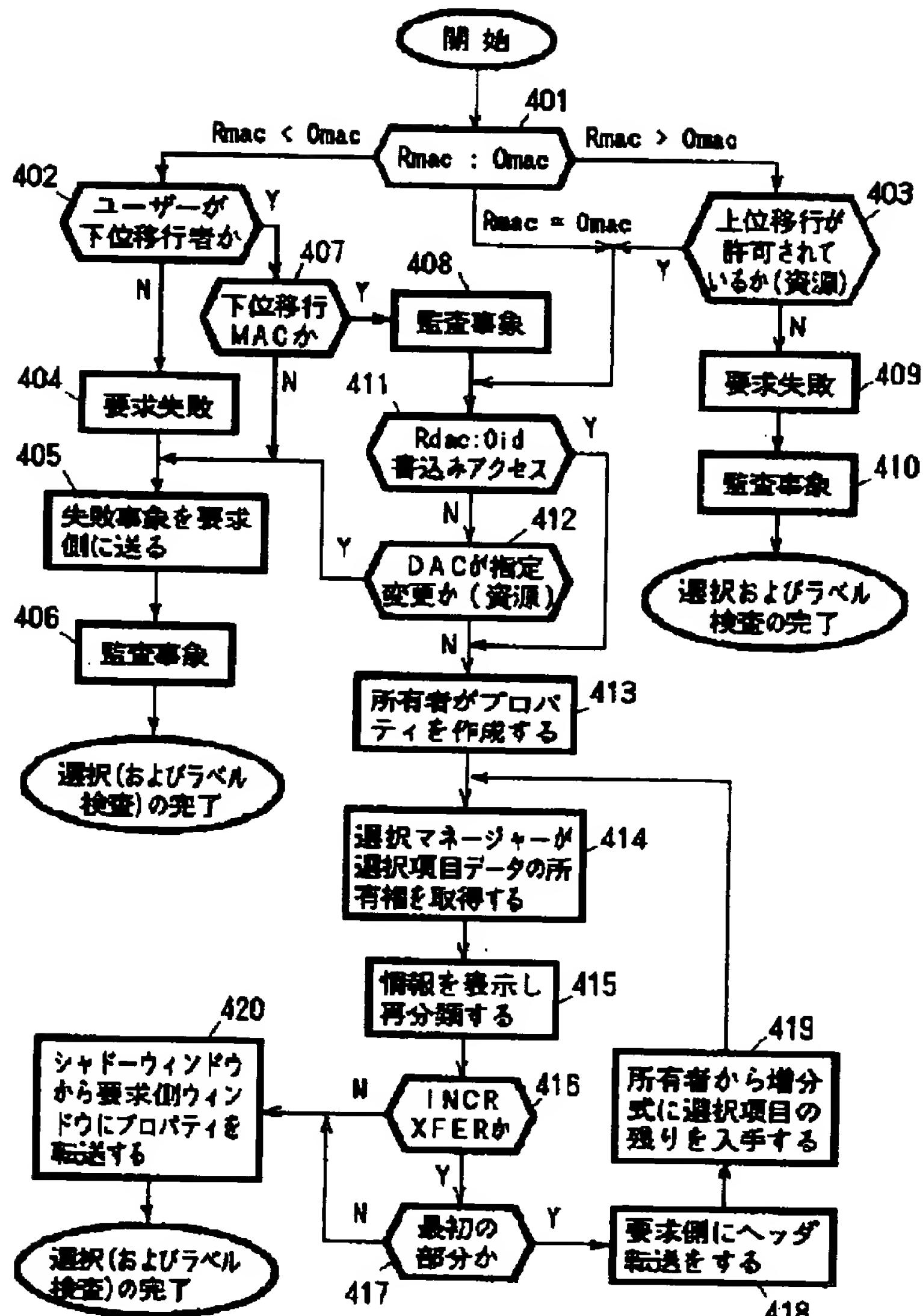
【図2】



【図3】



【図4】



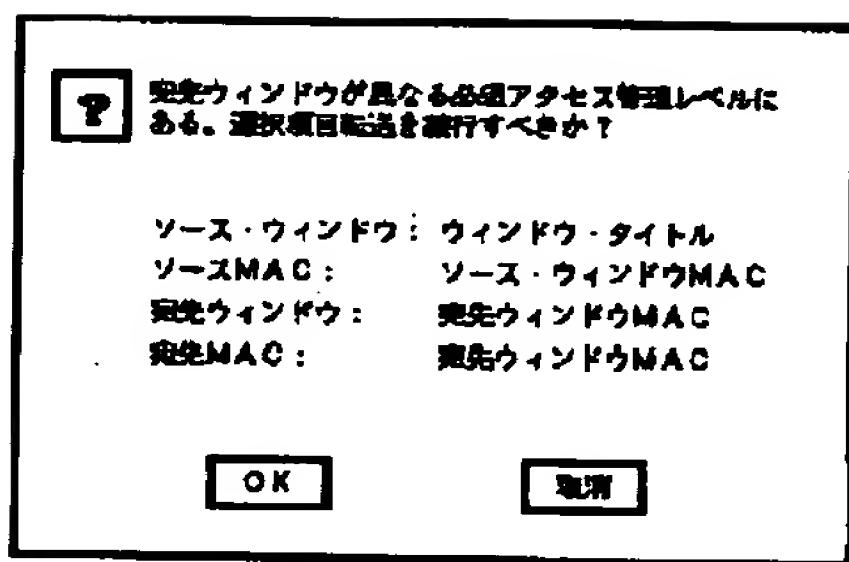
【図7】

データの所有者は要求側のウィンドウまたはプロパティに  
対する書き込みアクセスを持っていない。  
それでも実行するか？

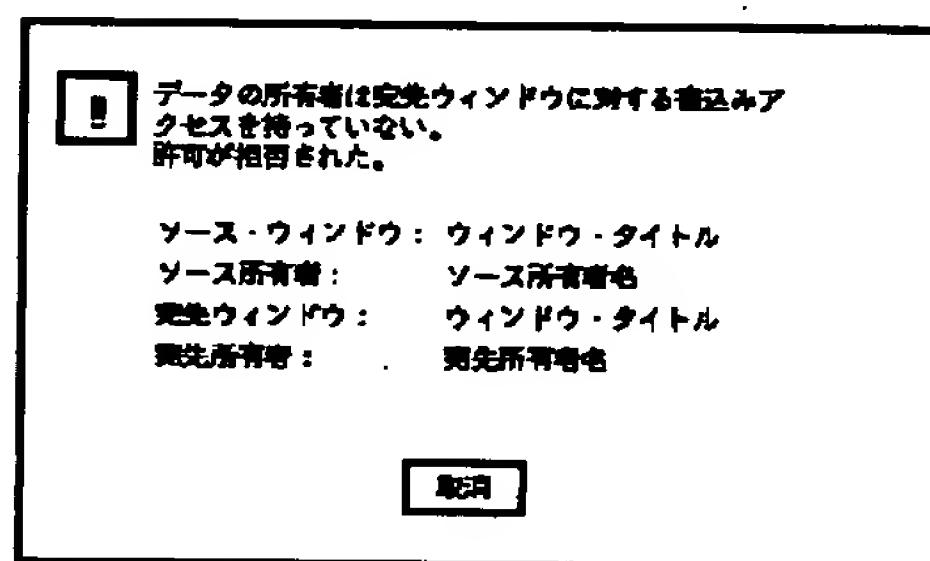
OK

取消

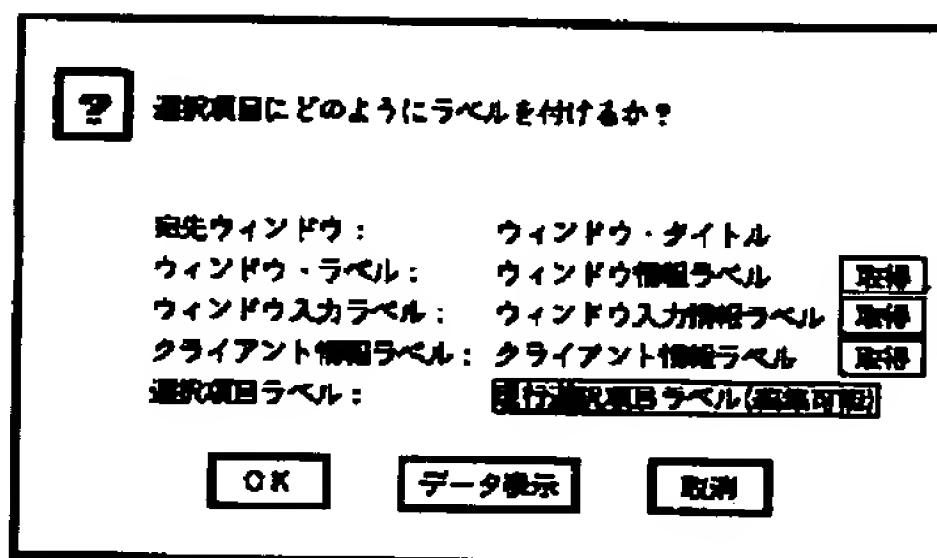
【図6】



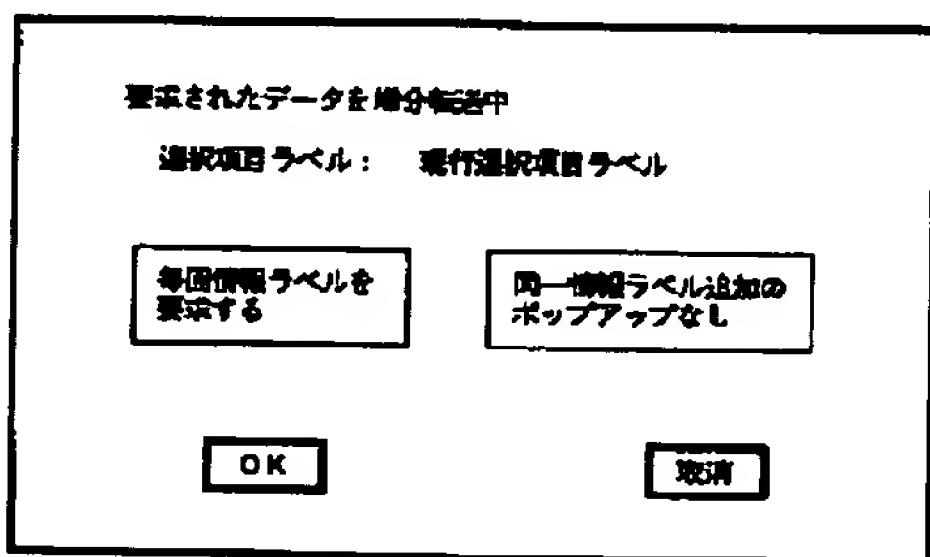
【図8】



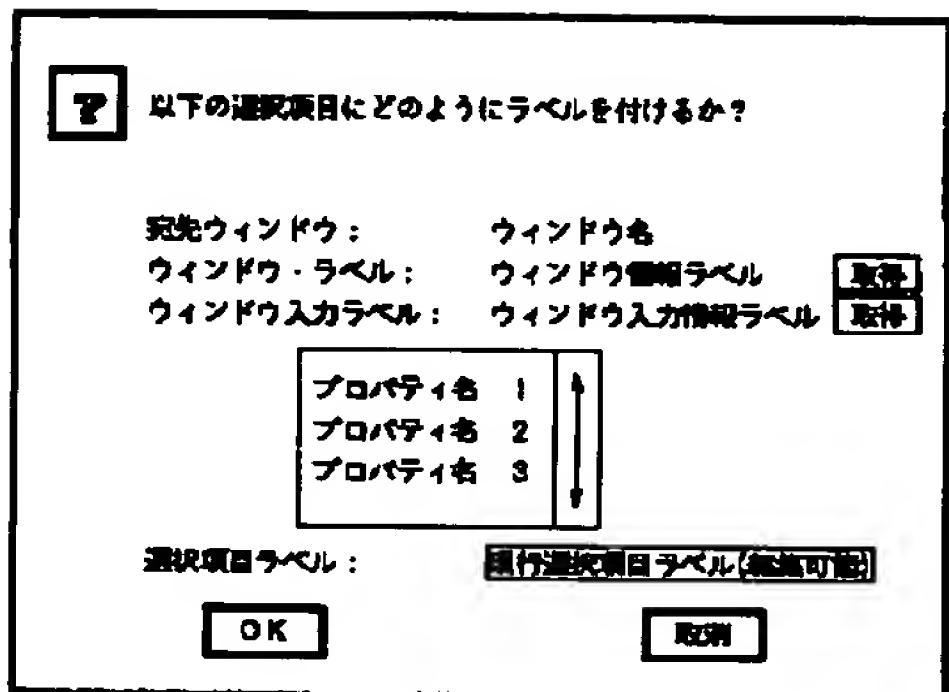
【図9】



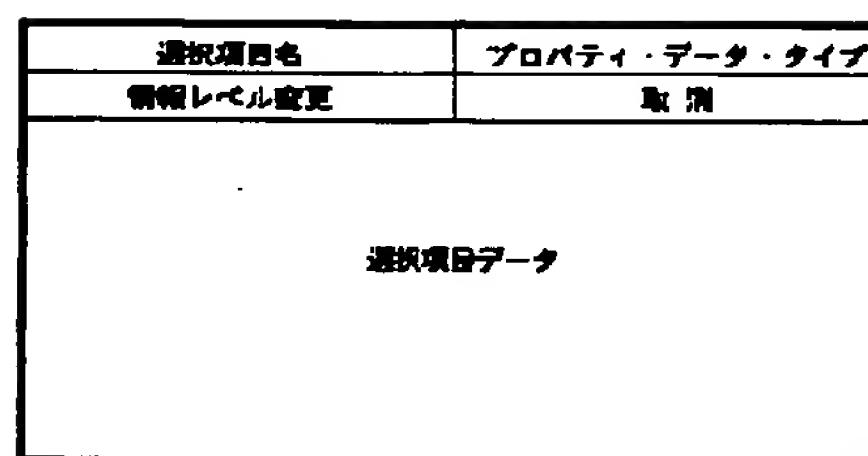
【図10】



【図11】



【図12】



フロントページの続き

(72)発明者 ムドゥムバイ・ランガナタン  
アメリカ合衆国20905 メリーランド州シ  
ルバー・スプリング スタートヴァント・  
ストリート 14405

(72)発明者 ジャネット・アン・クジーニ  
アメリカ合衆国21793 メリーランド州ウ  
オーカーズヴィル グレープ・クリーク・  
ロード 8998